BOIES SCHILLER FLEXNER LLP
David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel.: (914) 749-8200
dboies@bsfllp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Alison L. Anderson, CA Bar No. 275334
M. Logan Wright, CA Bar No. 349004
2029 Century Park East, Suite 1520
Los Angeles, CA 90067
Tel.: (213) 995-5720
alanderson@bsfllp.com
mwright@bsfllp.com

SUSMAN GODFREY L.L.P.
Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
Ryan Sila (admitted pro hac vice)
One Manhattan West, 50th Floor
New York, NY 10001
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com
rsila@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN
John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
Michael F. Ram, CA Bar No. 104805
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
mram@forthepeople.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No.: 3:20-cv-04688-RS

[PROPOSED] ORDER DENYING GOOGLE'S MOTION FOR SUMMARY JUDGMENT

The Honorable Richard Seeborg

[PROPOSED] ORDER

Plaintiffs Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn Harvey ("Plaintiffs") assert three claims against Google: (1) invasion of privacy; (2) intrusion upon seclusion; and (3) violation of California's Computer Data Access and Fraud Act ("CDAFA"). Plaintiffs contend that Google unlawfully collects, saves, and uses app activity data while people have turned off a Google setting called "Web & App Activity" or a subsetting that Google internally calls "supplemental Web & App Activity" (together, "(s)WAA"). The Court previously denied Google's motion to dismiss these three claims (Dkt. 109), and the Court previously granted Plaintiffs' class certification motion with respect to these three claims (Dkt. 352) subject to the Court's subsequent order on the class definitions (Dkt. 384).

Google now moves for summary judgment on all claims. First, Google argues that it is entitled to summary judgment on all claims on the basis that no reasonable juror could find that Google lacked consent, with Google arguing that its disclosures unambiguously disclose and establish consent for the at-issue conduct. Second, Google contends that it is entitled to summary judgment on the claims for invasion of privacy and intrusion upon seclusion on the basis that no reasonable juror could find that there was an objectively reasonable expectation of privacy, that Google's conduct is offensive, or that Google's conduct is intentional. Third, Google contends that it is entitled to judgment on all claims on the basis that no reasonable juror could find that Plaintiffs have been harmed. Fourth, Google contends that it is entitled to judgment on the claim for violation of the CDAFA on the basis that app developers consented to Google's conduct. For the reasons that follow, Google's summary judgment motion is **DENIED.**

LEGAL STANDARD

"The court must draw all reasonable inferences in favor of [Plaintiffs], including questions of credibility and of the weight to be accorded particular evidence." *Nat'l Fire Ins. v. Fed. Ins.*, 843 F. Supp. 2d 1011, 1014 (N.D. Cal. 2012) (Seeborg, J.). Summary judgment may be granted only if "the record taken as a whole could not lead a rational trier of fact to find for the non-moving party." *Matsushita Elec. Indus. Co. v. Zenith Radio*, 475 U.S. 574, 587 (1986). The Supreme Court

counsels "caution in granting summary judgment." *Consumer Fin. Prot. Bureau v. Nationwide Biweekly Admin., Inc.*, 2017 WL 11673197, at *2 (N.D. Cal. Feb. 6, 2017) (Seeborg, J.) (quotations omitted).

DISCUSSION

I. Consent

Google is not entitled to summary judgment on its express consent defense. As both parties acknowledge, express consent is a demanding defense, particularly at summary judgment. To succeed, the defendant must prove that it "unambiguously" discloses the "practice[s] at issue," which here is Google's collection, saving, and use of (s)WAA-off app activity data. *Brown v. Google LLC*, 2023 WL 5029899, at **7-8 (N.D. Cal. Aug. 7, 2023) (quotations omitted); *see also In re Google RTB Consumer RTB Consumer Privacy Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) ("In order for consent to be actual, the disclosures must explicitly notify users of the practice at issue." (quotations omitted)). A corollary to this rule is that the plaintiff's consent must be "'clearly and unmistakably stated.'" *Satterfield v. Simon & Schuster*, 569 F.3d 946, 955 (9th Cir. 2009) (quoting Black's Law Dictionary 59 (7th ed. 1999)). As the California Supreme Court has explained, consent is effective only if it is "voluntary." *Hill v. NCAA*, 7 Cal. 4th 1, 26 (1994). Google does not satisfy this burden. While Google has not separately moved for summary judgment regarding the "permission" element under the CDAFA (Cal. Penal Code § 502(c)(2)), the same analysis precludes any summary judgment on that element.

Google does not unambiguously disclose that it collects, saves, and uses app activity data when (s)WAA is off. Google contends that its disclosures explicitly represent that (s)WAA controls only whether Google associates app activity data with "personal information," but a reasonable juror could disagree. In discussing the (s)WAA controls, Google states that (s)WAA "saves your activity on … site, apps, and devices that use Google services," and that (s)WAA "must be on" to "let Google save" this information. In Google's Privacy Policy and the Android privacy menu, Google directs users to the (s)WAA settings with representations that users can "control what [Google] collects" or "choose the activities and info you allow Google to save."

These disclosures are amenable to the interpretation Plaintiffs advance: Google offers control over *whether* Google saves app activity data, not only where or how Google saves it.

Google contends that it unambiguously discloses its collection of (s)WAA-off data through its statement—after promising "control [of] what [Google] collects"—that when (s)WAA is on, activity is saved in the user's "Google Account." As Plaintiffs correctly point out, there are several problems with this argument. First, Plaintiffs have cited evidence establishing that users interpreted the same disclosures (including the reference to "Google Account") to mean that Google would not collect or save their app activity data. Second, the evidence establishes a triable issue as to whether an objectively reasonable user could interpret this to describe where Google saves data when (s)WAA is on, not *whether* Google saves data when (s)WAA is off. Third, Google's contentions are especially meritless given the pages on which this statement appears do not explain what a "Google Account" is, let alone disclose the at-issue conduct. And if the user goes searching for a definition, this is what they find attached to Google's Privacy Policy:

> **Google Account**
> You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

As the Court explained in prior orders, this is anything but clear. Dkt. 109 at 8. It describes how and why to create a Google Account, not what it means for user data to be "in" or "outside" of it. With a "definition" like this, a reasonable user could readily conclude (as Plaintiffs contend) that when Google collects data about their activity, that data is part of their "Google Account." A reasonable user might conclude that however Google tracks and accounts for their activity, regardless of the precise identifier used, that is part of their "Google Account."

Summary judgment is especially unwarranted given the evidence produced in discovery indicating that many users understood that Google with its (s)WAA disclosures promised control over whether Google collects and saves app activity data. In user comprehension studies conducted

by Google, users responded that they interpreted the Google disclosures to mean that Google would not collect data when (s)WAA is off. These findings are supported by expert opinion, including that Google's disclosures include features called "dark patterns" that are known to conceal privacy risks from users. There is also evidence suggesting that Google's employees understood the Google disclosures to promise that Google will not collect (s)WAA-off data. Google's Chief Executive Officer Sundar Pichai also testified to Congress that Google's users "can clearly see what information *we have*—we actually show it back to them. We give clear toggles, by category, where they can decide *whether that information is collected, stored*." If Plaintiffs' understanding is shared by Google's own CEO, it is hardly unreasonable. Google may dispute Plaintiffs' interpretation of this evidence at trial, but at this stage "all reasonable inferences [must be drawn] in favor of [Plaintiffs]." *Nat'l Fire Ins.*, 843 F. Supp. 2d at 1014.

In light of this evidence, Google is not entitled to summary judgment. According to Google, class members should have understood that (s)WAA offers control only over an undefined "Google Account" that is somehow separate, should have navigated to other pages to determine what the "Google Account" is, should have looked past the above-quoted definition of the Google Account attached to the Privacy Policy, and should have instead pieced together: (a) a statement in the Privacy Policy that "[w]hen information is associated with your Google Account, we treat it as personal information" and (b) a statement in the "Key Terms" page that "personal information" means "information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account." Piecing together these different parts, Google now contends—contrary to the testimony of Plaintiffs, documents produced by Google, and various other evidence—that (s)WAA somehow unambiguously promises control only over data associated with certain personally identifying information. If that is what Google meant, it could have said so clearly. Google offers no evidence that users actually piece together these cherry-picked statements in the way it now advocates. There is a substantial amount of evidence cited by Plaintiffs suggesting the opposite, including

admissions by Google employees. A reasonable juror could reasonably credit the evidence cited by Plaintiffs and reject Google's labyrinthine analysis of various pieces of different disclosures.

Summary judgment is also denied because a reasonable juror could reject Google's consent defense for two additional reasons. First, a reasonable juror could conclude based on the evidence presented that Google violates its representations even as Google interprets them. Plaintiffs have offered substantial evidence that the (s)WAA-off app activity data Google saves constitutes "personal information." This data is saved with identifiers that Google creates and manages, as well as additional information such as IP addresses. Google's identifiers are unique to each class member's mobile device, which constitutes an online identity. Plaintiffs have offered expert and documentary evidence that these Google identifiers are used to "personally identif[y]" users, including to build marketing profiles and track the effect of its advertisements on user behavior. Plaintiffs have also offered documentary evidence that Google considers its unique device identifiers to be personally identifying. A reasonable juror could readily agree that the (s)WAA-off app activity data collected by Google is "personal information." *See also In re Google RTB Consumer Privacy Litig.*, 606 F. Supp. 3d 935, 944 (N.D. Cal. 2022) (holding that "IP address" and "unique device identifier" "fall[] within the broad definition of personal information, as defined under both California law and in Google's privacy policy") (quotations omitted); Cal. Civ. Code § 1798.140(v)(1)(A) (defining personal information to include "[i]dentifiers such as a … unique personal identifier, online identifier, Internet Protocol address … or other similar identifiers"); 16 C.F.R. § 312.2 (defining "personal information" under the Children's Online Privacy Protection Act to include "[a] persistent identifier that can be used to recognize a user over time and across different Web sites or online services" such as "an Internet Protocol (IP) address … or unique device identifier".

Second, a reasonable juror may also reject Google's consent defense on the basis that any such consent is not voluntary under California law. In *Hill*, the California Supreme Court explained that consent may be considered "involuntary" if the "consequence" of refusal is exclusion from "a government benefit or an economic necessity that society has decreed must be open to all." 7 Cal.

4th at 42. Applying this logic, courts have concluded that when employment or participation in extracurricular activities is conditioned on drug testing, consent may be lacking. *See Hansen v. Cal. Dept. of Corrs.*, 920 F. Supp. 1480, 1505 (N.D. Cal. 1996) (holding consent involuntary as a matter of law); *see also Brown v. Shasta Union High Sch. Dist.*, 2010 WL 3442147, at **9-13 (Cal. App. Div. Sept. 2, 2010) (affirming preliminary injunction). In this case, a reasonable juror may conclude that any consent is not voluntary for two reasons. First, a reasonable juror may conclude that the Firebase and Google Mobile Ads SDKs are so ubiquitous that use of a mobile device is effectively conditioned on submission to Google's surveillance. Second, a reasonable juror may also conclude that in today's world, use of a mobile device is a "necessit[y], not [a] luxur[y]." Dkt. 352 at 13.

II. Invasion of Privacy and Intrusion Upon Seclusion

Google also is not entitled to summary judgment on Plaintiffs' claims for invasion of privacy and intrusion upon seclusion. To succeed on these claims, Plaintiffs must prove that "(1) there exists a reasonable expectation of privacy, and (2) [Google's] intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). For the intrusion upon seclusion claim only, Plaintiffs must also prove that Google acted intentionally. *See Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286-87 (2009) (describing this as an element of intrusion upon seclusion, but not mentioning it with respect to invasion of privacy). A reasonable juror could find in Plaintiffs' favor on each element.

A. Objectively Reasonable Expectation of Privacy

A reasonable juror could conclude that Google set an objectively reasonable expectation of privacy for many of the same reasons that it could find that Google lacked consent. Plaintiffs have offered substantial evidence supporting their interpretation of Google's disclosures—that (s)WAA should stop Google from collecting, saving, and using app activity data. Google offers only two additional arguments, both of which are meritless.

First, Google argues that users cannot reasonably expect that they can turn off mobile advertising by flipping a switch. That is not the basis for Plaintiffs' claims. Plaintiffs allege that

Google promised that it would not collect, save, or use (s)WAA-off data. A reasonable juror could conclude that it is reasonable to expect that Google will operate its advertising business without breaking that promise. A reasonable juror may decide not to give Google a free pass simply because it offers advertising services. In any event, Google offers no evidence that users understand that Google must collect and save (s)WAA-off data to serve advertisements.

Second, Google argues that users cannot have a reasonable expectation of privacy in pseudonymous data. The authorities upon which Google relies only reference *anonymous* data, not pseudonymous data. *See, e.g.*, *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021). As Google's witnesses concede, *pseudonymous* data can be linked to a person, whereas anonymous data cannot. Moreover, users may have an expectation of privacy in even *anonymous* data, especially when the defendant represented that it would not collect that data, or when the data can be de-anonymized. *See Brown v. Google LLC*, 2023 WL 5029899, at *5, *19 n.39 (N.D. Cal. Aug. 7, 2023) (denying summary judgment because "the reason Google has access to [class members'] anonymous, aggregated data [was] through the collection and storage of information from [their] private browsing history without consent"); *Wesch v. Yodlee*, 2021 WL 1399291, at *3 (N.D. Cal. Feb. 16, 2021) (holding that plaintiffs could have a "reasonable expectation of privacy in anonymized, aggregated data" because "it would only take a few steps to identify the individual Plaintiffs"); *see also In re Google Referrer Header*, 465 F. Supp. 3d 999, 1009-10 (N.D. Cal. 2020) ("[I]nformation need not be personally identifying to be private."). Finally, and as previously explained, Plaintiffs have presented sufficient evidence for a reasonable juror to conclude that (s)WAA-off data is personal information.

B. Highly Offensive

A reasonable juror could also conclude that Google's conduct is highly offensive. This element "essentially involves a policy determination as to whether the alleged intrusion is highly offensive under the particular circumstances." *Safari Club Int'l v. Rudolph*, 862 F.3d 1113, 1127 (9th Cir. 2017) (quotations omitted). The law "requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's

motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606. "A judge should be cautious before substituting his or her judgment for that of the community." *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016).

In this case, a number of considerations weigh in Plaintiffs' favor. For example, Plaintiffs offer evidence that Google's "own officials recognized these practices as a problematic privacy issue." *Facebook Tracking*, 956 F.3d at 606; *see also Brown*, 2023 WL 5029899, at *20 (denying summary judgment because of "evidence that Google's own employees found the data collection problematic"). Plaintiffs also offer evidence that the data Google collects is "vast and sensitive." *Brown*, 2023 WL 5029899, at *20. A person's activity on apps may reveal intimate details, such as their medical problems, sexual orientation, religious beliefs, and political leanings. Plaintiffs also offer evidence that Google collects data for its own independent benefit, including for use with other Google products. Google chooses not to collect other types of (s)WAA-off data if it is not valuable, but it chooses to collect sensitive app activity data to generate hundreds of millions of dollars in profits.

Google contends that its conduct is not highly offensive on the basis that it does not save identifying information. As previously explained, that is a genuinely disputed fact. And in any event, that single factor is not determinative. *See Brown*, 2023 WL 5029899, at *20 (denying summary judgment even with respect to purportedly anonymous data). The law requires a "holistic consideration" of the facts (*Facebook Tracking*, 956 F.3d at 606) and "California tort law provides no bright line" (*Hernandez*, 47 Cal. 4th at 287) (quotations omitted). Whether Google's conduct was highly offensive is an issue for the jury to decide.

C. Intent

A reasonable juror could also conclude that Google acted with the requisite intent, which is an element only of the intrusion upon seclusion claim. *See Hernandez*, 47 Cal. 4th at 286-87 (describing this as an element of intrusion upon seclusion, but not mentioning it with respect to invasion of privacy). For that claim, Plaintiffs must prove that Google intended to cause the

"'consequences of [their] act[s]'" or that they knew those consequences were "'substantially certain to result.'" *Marich v. MGM/UA Telecomms., Inc.*, 113 Cal. App. 4th 415, 422 (2003) (quoting Restatement (Second) of Torts § 8A). The existence of any intent is also a disputed issue that should be decided by the jury. Plaintiffs have presented evidence indicating that Google knowingly wrote and disseminated code that allowed Google to collect the at-issue (s)WAA-off app activity data. Plaintiffs have also presented evidence that Google knew that its disclosures gave rise to a reasonable expectation of privacy, acknowledging that there is a "real problem" with users expecting Google to not collect data when (s)WAA was off. The question of whether Google acted intentionally is a question to be decided by the jury.

III. Harm and Damage or Loss

Google's motion is also denied regarding the issues of harm and damage or loss. Based on the evidence presented by Plaintiffs, a reasonable juror could readily find harm and, under the CDAFA, "damage or loss." Cal. Penal Code § 502(e)(1). The evidence supports a finding of five different types of harm.

First, the reasonable juror could find injury to their right to privacy based on Google's surreptitious collection, saving, and use of app activity data. *See Facebook Tracking*, 956 F.3d at 598 ("[V]iolations of the right to privacy have long been actionable at common law." (quotations omitted)).

Second, a reasonable juror could find harm or damage or loss based on evidence that Google took class members' valuable data and then exploited it for profit. *See id.* at 600-01 (allegation that defendant "profited from [plaintiffs'] valuable data" amounts to a "violation" of a "state law interest … sufficient to establish standing to bring their claims for CDAFA violations").

Third, a reasonable juror could find harm or damage or loss because "Google failed to pay for collected data despite there being a market for it." Dkt. 352 at 12 n.3 (quotations omitted); *Facebook Tracking*, 956 F.3d at 600 (data "carr[ied] financial value" and plaintiffs were uncompensated); *Brown*, 2023 WL 5029899, at *19 (denying summary judgment where "there is a market for [class members'] data" based on a "misappropriat[ion]"-type injury).

Fourth, a reasonable juror could find harm or damage or loss because of evidence that Google's collection of data depletes class members' devices of battery and bandwidth. *See In re Carrier IQ*, 78 F. Supp. 3d 1051, 1065-67 (N.D. Cal. 2015).

Fifth, a reasonable juror could find harm or damage or loss because Google violated its representations, and therefore class members did not receive the "benefit of their bargain." *McClung v. AddShopper, Inc.*, 2024 WL 189006, at *2 (N.D. Cal. Jan. 17, 2024).

IV. Permission Under the CDAFA

Google's final argument is meritless. Google cannot invoke developer consent to escape liability from an otherwise viable claim under the CDAFA. "Ninth Circuit precedent . . . makes clear that [permission] is something that only the owner of the computer or similar authority can provide." *United States v. Thompson*, 2022 WL 834026, at *3 (W.D. Wash. Mar. 21, 2022) (collecting cases). If "authorization to access a computer has been affirmatively revoked," like by turning (s)WAA off, then the defendant "cannot sidestep the statute by going through the back door and accessing the computer through a third party." *United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016); *Sols. Team, Inc. v. Oak Street Health, MSO, LLC*, 2018 WL 11432145, at *9 (N.D. Ill. Mar. 5, 2018) ("Even when another party has rights to data stored on a computer, authorization . . . must be provided by the owner of the computer.").

The authorities upon which Google relies are not to the contrary. Unlike in those cases, a reasonable juror in this case could readily find that Google received an express signal that class members do *not* give permission to access their devices or take, copy, or use their data. And unlike in the cases cited by Google, Plaintiffs have presented evidence that Google *does* use (s)WAA-off app activity data to serve its own independent purposes, not just those of app developers. Moreover, Google's cases concern a distinct law, the California Invasion of Privacy Act, which does not control the question of permission under the CDAFA.

CONCLUSION

For these reasons, Google's motion for summary judgment is **DENIED.**

IT IS SO ORDERED.

DATED: _____

_____

Honorable Richard Seeborg
Chief United States District Judge